TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"
presented to you by MACRO Systems LLC

Macro Systems, LLC.

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems.
One call does it all!"

Howard F. Cunningham, Jr.
President and Founder

SERVING THE METRO DC AREA FOR OVER 20 YEARS

Volume 19, Issue 11, November, 2019
Fairfax, Virginia

Inside This Issue...

2013 SMB 150

HOWARD CUNNINGHAM
Top Channel Influencer

Connect With Us!

The Threat of URL Manipulation

Chances are that you know what a URL is, but if you don't: it is the address of a website. It usually starts with "http//:" or "https://" and directs the Internet browser on where the user would like to surf. What you need to always be aware of is that these days a threat can be created by manipulating the URL.

The URL

At the beginning of the URL is the protocol, which tells the computing network which language is being used. For most Internet-based directions, the protocol will be HTTP, for Hypertext Transfer Protocol. Other protocols you'll see include File Transfer Protocol (FTP), News, and Mailto. The next part is the ID and password. Since most people don't want their login credentials exposed, they leave this information out of the URL. Safety first. The following part of the URL is the server name. The server name gives users a path to access information stored on specific servers whether they are loaded through a domain or through the IP address associated with that server.

The fourth part of the URL is the port number. This number is associated with the services on the server and tells them what type of resources are being requested. The default port is port 80, which can be left off the URL as long as the information that is being requested is associated with port 80. You'll often not see the port number during day-to-day surfing, because most legitimate sites use the standard port 80. The final part of the URL is what is called the path, which provides direct access to the resources found tied to the IP (or domain).

Manipulating the URL

When a hacker wants to manipulate a URL, they do so by changing parts of the URL to test access. Since most users navigate a website through traditional means (that they use the links provided on the website) sometimes hackers can locate vulnerabilities by a trial and error approach. By manipulating the parameters to try different values, hackers can test directories and file extensions randomly to find the resources they are after. This provides access to resources that usually wouldn't be available and would otherwise be protected. Modern hackers have tools that allow them to automate these penetrations, making it possible to test a website (and more specifically, find vulnerabilities) in seconds. With this method, these hackers can try searching for directories that make it possible to control the site, scripts that reveal information about the site, or for hidden files.

Directory traversal attacks, also known as path traversal attacks, are also popular. This is where the hacker will modify the tree structure path in a URL to force a server to access unauthorized parts of the website. On vulnerable servers, hackers will be able to move through directories simply.

What You Can Do?

By securing your network against URL attacks, you are removing major vulnerability points. One thing you can do is to ensure that all of your Internet-based software is updated and patched with the latest threat definitions. In doing so you gain a lot more control over your network and data.

The IT experts at Macro Systems can help you keep your business' IT infrastructure from working against you. Call us today at 703-359-9211 for more information about how to maintain your organization's network security.